

**MEMORANDUM OF UNDERSTANDING**  
**BETWEEN**  
**THE DEPARTMENT OF ADMINISTRATIVE SERVICES**  
**AND**  
**THE CONNECTICUT HEALTH INSURANCE EXCHANGE**

## TABLE OF CONTENTS

Recitals.....	4
1. Background.....	5
2. Purpose and Scope.....	5
3. Definitions.....	5
4. Actions, Responsibilities and Obligations.....	6
4.1    BEST Responsibilities.....	6
4.2    Exchange Responsibilities.....	6
5. Terms.....	7
6. Communication.....	7
7. Financials and Chargeback.....	8
8. Invoicing.....	8
9. Service Areas.....	9
9.1    Core Infrastructure Services.....	9
9.1.1    Platform Services.....	9
9.1.2    Data Hosting Services.....	11
9.1.3    Application Services.....	14
9.1.4    Server Management, Backups and Recovery.....	17
9.1.5    Storage Area Network Services.....	19
9.1.6    Network Services.....	20
9.1.7    Exchange Security Services.....	21
9.1.8    Infrastructure Security Services.....	22
9.1.9    Help Desk and Operational Services.....	23
9.1.10    Change Management Process & Procedures.....	24
10. Confidentiality Definitions.....	26
11. Protection of Confidential Information.....	27
11.1    Duty to Protect.....	27
11.2    Data Security Program.....	27
11.3    mandatory Reporting.....	27

11.4	Protection Plan and Credit Monitoring.....	28
11.5	Responsibility of Contractors.....	28
11.6	Impact on HIPAA.....	28
12.	Modification and Termination.....	28
12.1	Termination for Material Breach.....	28
12.2	Termination for Convenience.....	29
12.3	Loss of Funding.....	29
13.	Entire Agreement/Modification.....	29
14.	Intellectual Property.....	29
15.	Insurance.....	30
16.	Application of Law.....	30
17.	Language of Execution.....	30
18.	Multiple Counterparts.....	30
	APPENDIX A – CMS Security COntrols.....	32
	APPENDIX B – COMPLIANCE WITH IRS PUB 1075.....	46

TABLE OF FIGURES

Figure 1 – Service Level Objectives.....	11-11
Figure 2 - Latency Measurement.....	13
Figure 3 - Service Credit Calculation.....	14
Figure 4 - Hardware.....	15-16

**MEMORANDUM OF UNDERSTANDING**

**BETWEEN**

**THE DEPARTMENT OF ADMINISTRATIVE SERVICES**

**AND**

**THE CONNECTICUT HEALTH INSURANCE EXCHANGE**

This Memorandum of Understanding ("MOU"), is entered into by the Connecticut Health Insurance Exchange (hereinafter "Exchange") established under Conn. Gen. Stat. §38a-1080 *et seq.* and the Department of Administrative Services (hereinafter "DAS") on behalf of the Bureau of Enterprise Systems and Technology (hereinafter "BEST") (collectively, the "Parties") under the following terms and conditions.

**WHEREAS**, the purpose of the Exchange as set forth in Conn. Gen. Stat. §38a-1080, *et seq.* is to implement the Affordable Care Act (hereinafter "ACA") in Connecticut and reduce the number of Connecticut residents without health coverage, by assisting individuals in gaining access to health care by providing comparable and easily understandable information about health insurance options and health benefit programs, and by qualifying individuals for federal tax subsidies, or health benefit programs as appropriate; and

**WHEREAS**, the Exchange is authorized and directed to develop a web portal and a single shared eligibility system that will be used by both the Exchange and the Department of Social Services (hereinafter "DSS") in informing Connecticut residents about their options, and qualifying Connecticut residents for financial assistance and benefit programs, as appropriate; and

**WHEREAS**, to develop and operate the web portal and single stream lined eligibility system, the Exchange requires these specific services: Hardware hosting services, application hosting, platform services, server management, backups and recovery, storage area network services, infrastructure security services, helpdesk and operational services; and,

**WHEREAS**, BEST provides such quality information technology (IT) services and solutions to state customers to provide the most cost-effective solutions to facilitate and improve the conduct of business for Connecticut; and

**WHEREAS**, both the Exchange and the Parties recognize the need for a coordinated effort to: implement the requirements of the ACA; attain economies of scale in system development and maintenance; facilitate required data transfers between state agencies, the Exchange and the federal data services hub; and maintain Exchange, state and federal data in a secure environment in strict compliance with HIPAA and IRS standards and all other federal and state laws and regulations governing the privacy and confidentiality of data.

## **NOW THEREFORE IT IS HEREBY MUTUALLY AGREED THAT:**

BEST will provide IT services, software and hardware and Exchange shall pay for such services, software and hardware as set forth in this Agreement and the Appendices attached hereto.

### **1. BACKGROUND**

The Exchange is required by Conn. Gen. Stat. §38a-1080, *et seq.* and the ACA to facilitate healthcare insurance selection and to determine eligibility for Advance Premium Tax Credits and Cost Sharing Reductions and for Medicaid and CHIP in compliance with the ACA. In support of this requirement, the Exchange is developing an integrated eligibility solution and a web portal to qualify individuals and small businesses for enrollment in the Qualified Health Plans offered through the Exchange or in DSS programs, as applicable.

BEST provides quality information technology (IT) services and solutions to state customers. BEST has assisted the Exchange in planning its integrated eligibility solution and is willing to create and support the core IT infrastructure for the Exchange. Specifically BEST is willing to: procure hardware and software for the Exchange for user acceptance testing (UAT), staging and production and is also willing to: build, install the vanilla software and configure software in user acceptance testing (UAT); build, configure and maintain staging and production environments to support the Integrated Eligibility Solution; and provide services to the Exchange as further defined within this Agreement and Appendices.

### **2. PURPOSE AND SCOPE**

BEST will create and support the core infrastructure for the Exchange and host the Exchange's Integrated Eligibility system. This includes the procurement, build, installation, and maintenance of the following environments to support the Exchange: user acceptance testing, staging, and production. The core infrastructure is defined as including but not limited to: network services; application services; data services; platform services; security services; operational services; planning and architecture; and, communications and collaboration. It is possible that due to the complex nature of setting up a state exchange there are services and/or support needs that are not defined herein. If that assumption proves valid, the Exchange and BEST will work together to share ownership to execute the required component and/or functionality, and will amend this memorandum of understanding as required.

### **3. DEFINITIONS**

- Exchange – Connecticut Health Insurance Exchange
- BEST – Bureau of Enterprise Systems and Technology
- ACA – Affordable Care Act
- State – State of Connecticut
- DAS – Department of Administrative Services
- DSS – Department of Social Services
- CMS – Centers for Medicare and Medicaid Services

- IRS – Internal Revenue Service
- HIPAA – Health Insurance Portability and Accountability Act of 1996 as amended
- MOU - Memorandum of Understanding
- OEM - Original Equipment Manufacturer
- SAN - Storage Area Network
- 50ns - Scope, Schedule, Budget, Quality, and Benefits

## **4. ACTIONS, RESPONSIBILITIES AND OBLIGATIONS**

### **4.1 BEST RESPONSIBILITIES**

BEST shall undertake the following activities during the duration of the MOU term.

1. Provide the following services to support the Integrated Eligibility program for the Exchange:
  - Platform Services
  - Hardware and Data Hosting Services
  - Application Hosting
  - Server Management, Backups and Recovery
  - Storage Area Network (SAN) Services
  - Network Services
  - Infrastructure Security Services (Firewall, Intrusion Detection Service (IDS), Intrusion Prevention Service (IPS))
  - Help Desk and Operational Services related to infrastructure
  - Change Management Process & Procedures.
2. Support and lead infrastructure procurement, setup/build activities.
3. Install hardware.
4. Install and configure software in accordance to Deloitte Application Install Playbook Document.
5. Establish User Acceptance Testing (UAT), Staging, and Production environments to support the Exchange.
6. Support and partner with the Exchange to ensure a successful Integrated Eligibility customer experience.
7. Share with the Exchange the infrastructure developed to support the Integrated Eligibility Solution for the Exchange.
8. Provide infrastructure security services in compliance with HIPAA and the CMS Security Control Detail as set forth in Appendix A, hereto, and IRS Compliance Standards as set forth in Appendix B, hereto, and all applicable federal and state laws and regulations and program guidelines.
9. Review and approve all documentation evidencing BEST performance of services as set forth in the Scope of Work; invoice for such services according to the terms of this MOU; and monitor BEST compliance with the MOU.

### **4.2 EXCHANGE RESPONSIBILITIES**

The Exchange shall undertake the following activities during the duration of the MOU term:

1. Reimburse allowable expenses within 45 day according to the terms and conditions set forth in Appendix C to this MOU.
2. Ensure BEST has a single point of contact from the Exchange IT Systems and Operations Team who has decision authority.
3. Support and partner with BEST to ensure a successful Integrated Eligibility customer experience.
4. Review within 30 days the BEST services used, with the understanding that – if there are any additional charges to BEST for these services from BEST's vendors – these additional charges will be billed to the Exchange within 30 days of their presentation to BEST.
5. Retain primary responsibility for all application functions, including but not limited to overall system performance, system and application design changes and documentation, timely notification of required changes, and business volume modeling that relates to system performance and architecture.
6. Ensure BEST's and the Exchange's adherence to HIPAA, CMS Security Control Detail as set forth in Appendix A, hereto, and the IRS Compliance Standards as set forth in Appendix B, hereto, and all applicable federal and state laws and regulations and program guidelines.
7. Review and approve all documentation evidencing the Exchange's performance of services as set forth in the Scope of Work and monitor the Exchange's and BEST's compliance with the MOU.

## **5. TERMS**

This MOU shall be effective upon the last date of execution and shall continue until terminated in compliance with Section 12 of this MOU.

## **6. COMMUNICATION**

### **6.1 Notices**

Any and all correspondence made or notices to be sent or required to be made under this MOU shall be in writing, signed by the Party giving such notice (claim or demand) and shall be delivered personally, or by facsimile transmission or by registered mail, to the other Parties at its addresses set forth herein below or at such other addresses as such other Parties may subsequently notify. All notices shall be deemed given when delivered, which includes facsimile transmissions.

#### ***Exchange***

*Telephone No: 860-757-5318*

*Address: 280 Trumbull St. Hartford, CT 06103*

*Attention: CIO Exchange*

*Telephone No: No: 860-757-5311*

*Address: 280 Trumbull St. Hartford, CT 06103*

*Attention: Assoc. Director IT Systems and Operations Exchange*

#### ***BEST***

*Telephone No: 860-622-6219*

*Address:*

*101 East River Drive, East Hartford, CT 06108*

*Attention: CIO BEST*

*Telephone No: 860-622-2494  
Address: 101 East River Drive, East Hartford, CT 06108  
Attention: Director of Operations BEST*

## **6.2 Public Announcement**

The release and contents of all public announcements (unless such disclosure is required under any applicable law) related to the MOU shall be subject to the prior written approval of each Party. In the event disclosure is required under any applicable law, such as, but not limited to the Freedom of Information Act (FOIA), the disclosing party shall notify the other party of the request, before disclosure, unless such notice is prohibited by law. The Exchange and the Parties further agree to cooperate and assist each other in responding to such disclosure requests.

## **7. FINANCIALS AND CHARGEBACK**

Collections for the BEST will be made through the BEST agreed upon rate structure. The BEST rate structure has been reviewed with Exchange as of March 1, 2013. This review defined the chargeback process from labor and variable rates into specific shared and bundled services. Bundled services have the potential of including direct labor, contracts, hardware, software and other direct costs required by BEST to provide technology services delivery for the associated centralized services.

The expectations for all billing methodologies are based on the following guiding principles:

- Rates must be equitable;
- Rates must be reasonable and competitive;
- Compliance requirements related to the State's IT practices, such as legal licensing of all software must be met.

The hardware and software maintenance contracts will continue to be paid by the cost center currently making payments. The decision of which hardware and software maintenance contracts are transferred to BEST will be made on a case-by-case basis in the future. Until a defined process is formally agreed to in writing BEST will hold the hardware and software licenses. BEST reserves the right to chargeback Exchange for additional volume tied additional usage as a result of supporting the Exchange application environment.

The Exchange and BEST are still working out the rate schedule for the agreed upon services as set forth in this Agreement. When the rate schedule is finalized, it will added as Appendix C to this Agreement. Appendix C which will incorporate the above principles must be signed by each party to this Agreement.

## **8. INVOICING**

BEST utilizes the Internal Services Fund financial model, which permits BEST to recover the costs of the service that it provides by charging for the usage of that service in a manner similar to a private enterprise but without the profit motivation.

Since BEST uses a metered ISP vendor service for Internet access, BEST will invoice Exchange for the total number of users and the data usage (Payload). Exchange team will track and report the number of users and the data payload in MB on a monthly basis to BEST and reimburse BEST for the number of users and payload usage (MB) so that BEST can payback the ISP vendors for the metered Internet usage service provided through BEST. Initial expectation is 1.5+ million users for the Exchange application. Exchange further agrees to pay BEST for any growth of users and/or growth in data usage in the future for the Exchange project. Exchange specifically recognizes that existing traffic or future growth may require the BEST team to expand their network backbone to 40GB to handle the Exchange application traffic. If expanded network backbone is required, Exchange recognizes that the reasonable costs of this expansion will be charged back to Exchange at an additional cost to the Exchange project.

BEST will continue to issue monthly billing amounts based upon the rate structure established at the time of billing. These invoices will be issued under the current practices. The summary page of the invoice service, will serve as the invoice to allow Inter-Governmental Transfers (IGT), which Exchange will utilize to process its payment to BEST using the state's accounting system. The Exchange may submit any billing inquires or requests for billing adjustments to the BEST by notifying the identified contact on the invoice.

As cost savings are identified, the costs to agencies will decrease on a case-by-case basis. For example, if services in a building were consolidated in one location, the lowered direct costs of doing so would be proportionally shared among the users of those servers. In another example, if BEST negotiates a lower rate for Virtual server licensing, then all impacted users will benefit. Under such an incremental change scenario, as further cost savings and services improvements are attained, service levels and reoccurring costs will tend to become more consistent.

## **9. SERVICE AREAS**

### **9.1 CORE INFRASTRUCTURE SERVICES**

#### **9.1.1 Platform Services**

##### **9.1.1.1 Service Definition**

Platform Services provide high performance, high volume, high availability, and server resources for a wide range of information technologies. These services are provided over a wide range of hardware and software operating systems.

The following are available within Platform Services:

- Statewide Data Center Facilities
- Mainframe Platforms (Server)
- Distributed Platforms (Server)
- Virtualization – Application Platforms

- Virtualization – Virtual Desktops
- Virtualization – Virtual Application Delivery
- Enterprise Storage Services (SAN, Tape, Disk, etc.);
- Desktop Services.

Platform Services will produce the following key benefits:

- 24 x 7 operation including real-time monitoring and fault management;
- Standard server platform technologies;
- Data retention and data recovery of Exchange critical data as defined by Exchange (both on and off-site storage);
- Secure and environmentally controlled data center environment;
- Automated production scheduling services
- Systems monitoring, Exchange business application monitoring, Exchange Batch job monitoring, performance and capacity management software tools; and
- Network print services, as applicable.

### 9.1.1.2 Service Level Objectives

Definition	<b>General System Availability</b> is defined as the service CPU, system memory, disks and peripherals up to the connection to the network. Availability is for the server or server-cluster that provides an Exchange-facing service and excludes scheduled maintenance.		
Pre-Scheduled Downtime Requirements	All pre-scheduled system downtime and maintenance, unless otherwise agreed upon in advance by Exchange, will occur as follows; <ul style="list-style-type: none"> <li>• For the systems with 24x7 requirements, all pre-scheduled maintenance shall be performance based on the change management process (defined below) and during agreed scheduled maintenance windows.</li> <li>• For systems having non-24x7 requirements, pre-scheduled maintenance shall be performed outside of the normal systems available timeframe.</li> </ul>		
<p><b>General System Availability Service Level Requirements</b>  <i>*BEST TRB approved 98.3% environment availability for the Exchange and ConneCT servers including Mainframe availability.</i>  <i>*BEST has defined maintenance windows on Sundays:</i></p> <ul style="list-style-type: none"> <li>• Sunday 5:00 a.m. – 7:00 a.m. three times a month</li> <li>• Sunday 5:00 a.m. – 9:00 a.m. one times a month</li> </ul> <p><i>These defined times for scheduled maintenance will not be included in the downtime per month or per year Service Levels as this is planned. Additionally, the below platform availability applies only to BEST infrastructure, it's understood that application level issues will have to involve Deloitte and will be within the scope of the below Service Level Availability.</i>  Downtime per month: 000d 12h 14m  Downtime per year: 006d 04h 55m</p>			
System Platform	Service Measure	Performance Target	Minimum Performance %
Mainframe O/S and Subsystems Mission Critical	Aggregate Availability	Fri-Thu, 00:00-24:00	98.30%
Windows Mission Critical	Aggregate Availability	Fri-Thu, 00:00-24:00	98.30%

Windows Others (Distributed)	Aggregate Availability	Fri-Thu, 00:00-24:00	98.30%
UNIX/Mission Critical	Aggregate Availability	Fri-Thu, 00:00-24:00	98.30%
UNIX Others (Distributed)	Aggregate Availability	Fri-Thu, 00:00-24:00	98.30%
QA/Test Systems and Servers	Aggregate Availability	BEST agrees to offer high available services during normal business hours and other periods as agreed upon	N/A

Figure 1 – Service Level Objectives

All System platforms include the following where applicable:

- Virtualization – Application Platforms, Virtualization – Virtual Desktops, Virtualization – Virtual Application Delivery;
- Enterprise Storage; and
- Desktop Services.

Performance percentage will be calculated from available system uptime records of critical devices. As BEST's incident management system and processes matures, the effort of the outage to Exchange will be calculated through trouble tickets or incidents logged into BEST's incident management system. The duration of every outage or service interruption will be captured. Service interruptions and outages will be reported back to Exchange on a monthly basis. Minimum performance percentages will be calculated by summing up the total number of minutes that the service was not available by each platform, subtracting that from the total number of minutes the system platform should have been available, then dividing by the total number of minutes the system should have been available. For example, support for the mainframe is expected to be available 24 hours a day, 7 days a week. The mainframe experiences a twenty-minute outage and another forty-minute outage later in the month, performance percentages would be calculated by taking the number of minutes available in a day (1,440) multiplied by the number of days in a month. Assuming thirty dates in the month, BEST's total number of available minutes would be 43,200. BEST would then sum the outages for the month (20+40), and calculate performance percentages as  $(43,200 - 60)/43,200$  which would equal 99.86%. In this case BEST would not meet its service level objective for that month. This process would be repeated for each severity level. In order for BEST to guarantee such high minimum performance levels, production hardware must be supported by the manufacturer and operating systems software must not be more than two versions old.

## 9.1.2 Data Hosting Services

### 9.1.2.1 Service Definition

Data Services provides the services and resources for Exchange Applications Data. The BEST Team provides these data services in a high volume, highly availability, and secure Data Center Facilities at the State of Connecticut. These services are provided over a wide range of hardware and software operating systems.

The following are available within Application Services:

- Enterprise Data Practices & Standards
- Enterprise Database Systems Management

- Data Reporting and Transparency
- Data Architecture and Design
- Database Administration and Design

BEST will be playing the role of an internal Hardware Service Provider. In this role, BEST will host and manage the infrastructure required to support business applications and will coordinate the support, maintenance, upgrades and administration of hardware and software with Exchange IT Systems and Operations Team. The Exchange will be responsible for requirements. The BEST will be responsible for systems design, build, and maintenance and system performance. The location of the technology implemented or the specific components used should not be of concern as long as all defined requirements as fully met. Systems will be centralized and consolidated where practical and distributed where required. Through the hosting model, BEST will combine hardware, software, networking technologies and technical expertise to provide superior performance, increased security and 24/7 availability as effectively and affordably as possible.

BEST will provide routine maintenance, backup and operating system administration duties for all equipment purchased or leased on behalf of Exchange. This stipulation may include, but is not limited to, implementing routine procedures to maintain and secure the integrity of Exchange infrastructure elements. Operating system administration duties may include, but are not limited to, installation of patches and operating system upgrades, responsibility for security including user administration, and providing liaison services with vendor support for maintenance, enhancement or upgrades to the existing systems.

## **9.1.2.2**

### **9.1.2.2.1 Service Level Objectives**

The BEST team will do their best to meet these Services Level Objectives for the Exchange Application.

#### **9.1.2.2.2 99.99% Network Uptime Requirement**

BEST intends to do their best to provide 99.99% availability for hardware part of the Exchange application. This footprint is comprised of the routers, firewalls, load balancers, and switches. For purposes of this document, the uptime does not include the dedicated Customer systems or Operating System layer. The Exchange Network will be deemed 'available' if the networking components are available and responding to BEST monitoring tools as designed and in a non-degraded manner (as evidenced in the BEST logs or BEST monitoring tool).

#### **9.1.2.2.3 99.99% Server Uptime Requirement**

For Servers deployed in the United States BEST intends to do their best to provide 99.99% availability of individual servers comprised of the Exchange environment. For purposes of this document, only failures due to hardware and hypervisor layers delivering individual servers are covered. The individual server will be deemed 'available' if the virtualization hardware and hypervisor layers delivering individual servers are available and responding to BEST monitoring tools as designed and in a non-degraded manner (as evidenced in the BEST logs or BEST monitoring tool).

#### **9.1.2.2.4 30 Minute Emergency Response Requirement**

BEST to do their best to provide support personnel intend to review and update any Help Desk Ticket submitted within 30 minutes for EMERGENCY Cases and within 120 minutes for all other cases. EMERGENCY Cases are considered any Case where a server is down and unavailable. BEST may reclassify, at its sole discretion, any Case misclassified as an Emergency Case, and such Case will not qualify for EMERGENCY treatment. Resolution and repair times vary, and therefore not covered under this document.

#### 9.1.2.2.5 <1 ms Latency Requirement

BEST intends to do their best to provide a latency of less than 1 ms for the transfer of data packets from one server to another within the BEST environment and within the same network (vLAN). Latency measurements are based on BEST standard monitoring systems. Latency between separate networks (vLAN's) is not covered under this document.

Description: Latency SLA is measured as the roundtrip response time from BEST to Exchange hardware across the BEST provided connection.

Measurement:

Latency	$\frac{\sum (\text{ICMP Packet Response Timestamp} - \text{ICMP Packet Sent Timestamp})}{\text{Total Number of ICMP Packets}}$
---------	--

Figure 2 - Latency Measurement

The Latency SLA measurement includes all elements between the Management Router (or BEST power path, as appropriate) and the Remote Access CPE. The Latency measurement is the average response time of a 32 byte ICMP PING packet to complete a roundtrip traversal from the Management Router (or BEST power path, as appropriate) to the WAN interface of the Exchange CPE and thus includes the serialization delay of the WAN interface of the Exchange CPE. For Exchange sites using hardware-based IPsec VPN connections, the Latency SLA measurement is measured to the loopback interface of the remote VAS Customer Premise Equipment (CPE) device/hardware located at BEST. Periods of time when the circuit utilization is greater than 75% of its stated capacity, as measured using 99th percentile sampling will be excluded from the Latency SLA measurement.

#### 9.1.2.2.6 Service Credit Calculation Based on the Following Metrics

In the event of a failure to meet the Network Uptime Requirement, Server Uptime Requirement, or Application Uptime Requirement, the duration of such failure period will be considered downtime. In the event of failure to meet the Support Response Time, the duration of time beyond the allotted response time shall be considered response delay. In the event of failure to meet the Latency, the duration of time with latency equal to or exceeding 1 ms shall be considered latency degradation.

The intent of this section is to ensure BEST has controls in place to prevent undo negative impact to the BEST infrastructure which would in turn impact the Exchange application. This service credit will not take effect until more than resource only billing is occurring for example billing for more than resource staff/hours including or billing for bundled services.

Monthly Cumulative Response Delay (listed in minutes)	Monthly Cumulative Latency Degradation (listed in minutes)	Monthly Cumulative Downtime (listed in minutes)	Monthly Cumulative Application Downtime (listed in minutes)	Service Credits (% of monthly fee)
0 - 30	0 - 60	0 - 60	0 - 60	5%
31 - 120	61 - 120	61 - 120	61 - 120	10%
121 - 180	121 - 180	121 - 180	121 - 180	15%
181 - 240	181 - 240	181 - 240	181 - 240	20%
241 - 300	241 - 300	241 - 300	241 - 300	30%
301 - 360	301 - 360	301 - 360	301 - 360	40%
361 - 420	361 - 420	361 - 420	361 - 420	50%
421 - 480	421 - 480	421 - 480	421 - 480	60%
481 - 540	481 - 540	481 - 540	481 - 540	70%
541 - 600	541 - 600	541 - 600	541 - 600	80%
601 - 660	601 - 660	601 - 660	601 - 660	90%
660+	660+	660+	660+	100%

Figure 3 - Service Credit Calculation

### 9.1.3 Application Services

#### 9.1.3.1 Service Definition

Applications Services provides the services and resources to Host Applications in a high volume, highly available, and secure Data Center Facilities at the State of Connecticut. These services are provided over a wide range of hardware and software operating systems.

The following are available within Application Services:

- Enterprise Application Practices & Standards
- Application Hosting and Support
- Application Development
- Enterprise Content Management

### 9.1.3.2 Application Hosting Services

BEST will install, configure and support the User Acceptance Testing (UAT), Staging and Production Environments for Exchange Application. BEST will maintain and support the hardware and software for web servers, application servers, database servers, and network connectivity across these environments. BEST will also provide a disaster recovery environments and the physical infrastructure to enable Exchange applications to operation in a reliable and secure environment. The hardware and software comprising BEST standard configuration will change periodically according to typical refresh cycles, new contract awards and evolving technical standards. Exchange will be notified of changes via the Formal Change Management Process.

The below table outlines the initial hardware list, the current list will be documented and updated by Exchange and BEST, outside of this document. A current inventory list will be posted into the folder quarterly, where this MOU resides at Exchange.

The following tables are the inventory of hardware and software components that will be hosted in BEST environment: (As of December 18, 2012)

#### 9.1.3.2.1 Application Hosting Services

Product Name
Melissa Data
Adobe EchoSign
Adobe Livecycle Output ES3
Load Balancer - Content Services Switch (CSS)
Corticon
Corticon Development Studio
Dell Model # R910, 6 3.3 Ghz CPU, 36 Cores, 512 GB RAM
Dell PowerEdge R810
IBM DB2 Advanced Enterprise Server Edition
IBM DB2 Advanced Enterprise Server Edition with PureScale
IBM FileNet Business Manager Add-on Authorized Linux on System z user Value Unit License + SW Subscription & Support 12 months (supports 900 users)550
IBM FileNet Business Process Manager Add-on External User Linux on System z User Value Unit License + SW Subscription & Support 12 months (supports 10,000 users)8,000
IBM FileNet Compliance framework Authorized User Value Unit License + SW Subscription & Support for 12 months (supports 100 users)85
IBM Performance Tester
IBM Qradar Appliance
IBM System x3650 X5
IBM Tivoli (Monitoring)
IBM Tivoli Access Manager/Tivoli Identity Manager
IBM WebSphere Base Edition

Product Name
IBM Websphere DataPower
IBM WebSphere Enterprise Service Bus Registry Edition
IBM WebSphere Network Deployment
IBM XIV Total disk size 52 TB, 1 Disk Array
Red Hat Linux 6.2
Tibco Netrics v4.x
vCenter Server Standard, Instance
vCenter Site Recovery Manager Standard
Webtrends
Windows 2008 Server R2

Figure 4 – Hardware

### 9.1.3.3 Application Hosting Services – Patches, Changes, etc.

BEST will conduct business application impact and analysis before applying patches to hardware and/or software. BEST will upgrade and/or apply patches to the hardware and software for application/database hosting to maintain an Original Equipment Manufacturer (OEM) supported environment and will communicate these changes to Exchange. The timing of upgrades will be by mutual agreement between BEST technical staff and the Exchange IT Systems and Operations Team. BEST may contract these services to a vendor with the prior written approval of the BEST IT Manager or designee, Exchange is responsible for the cost of application code changes needed to stay compatible with the OEM supported environment.

BEST will perform all changes to staging and production application code and databases in conformance with the Change Management Procedures (below).

BEST will monitor operational status of the Exchange infrastructure and application and make recommendation for system tuning but will not invoke changes until approved in writing by the Exchange IT Systems and Operations Team.

BEST will monitor database performance and make recommendations for changes but will not invoke changes until approved in writing by the Exchange IT Systems and Operations Team.

All BEST technical support staff will accept and maintain the appropriate security and confidentiality requirements.

Although BEST staff and providers will normally be able to access the applications on a 24 hour basis, excluding maintenance hours, BEST support of the hosting environment for Exchange applications and database will be available during normal business hours. Normal business hours are Monday through Friday from 8:00 a.m. to 5:00 p.m. (Eastern Standard Time),

excluding state holidays. After normal business hours the BEST support staff is on call and problem response time is within four (4) hours.

### **9.1.3.4 Service Level Objectives**

#### **9.1.3.4.1 Database and Storage**

- The Exchange database will be implemented in IBM DB2 v10.x Database Management System (DBMS).
- Exchange Application & Database Server SAN Storage will be provided on the State's SAN Device
- Any future increase in number Users or Data Payload Size for the Exchange Application over time will result in BEST Chargeback Exchange team for any additional SAN Storage Disk, SAN Switch Fabric, and SAN Frame Additional Costs

#### **9.1.3.4.2 Performance/Availability**

- It is anticipated the Exchange application will meet average response time objectives set in the functional and technical requirements
- BEST maintenance activities will be coordinated with Exchange to provide minimal impact on the Exchange project schedule
- Maintenance activities (e.g., SAN upkeep, backup power, air conditioning, etc.) will be monitored and managed by the BEST
- BEST ISP vendors will be responsible for the Access Level of the Internet Service provided to Exchange

#### **9.1.3.4.3 End User Configurations**

- The Exchange base application uses a standard Web browser and will not require any client-side installation of application software.
- To utilize the application, TCP/IP compliant transmission protocol must be used (either by software or hardware)

### **9.1.4 Server Management, Backups and Recovery**

#### **9.1.4.1 Service Definition**

Service management, backup and recovery provide maintenance of server's hardware and software, redundant backups, scheduled and unscheduled maintenance, OEM adherence and recovery/building of an inoperable environmental component. These services are provided over a wide range of hardware and software operating systems.

The following are available within Service Management, Backup and Recovery Services:

- Climate controlled facility;

- Redundancy (power, routers etc.);
- Server maintenance performed during defined window;
- Application backups;
- Database backups;
- Locked server racks;
- Server and database recovery
- Disaster management plan;
- Apply patches

Service Management, Backup and Recovery Services will produce the following key benefits:

- Ensure stable and consistent environment
- 24 x 7 operation including real-time monitoring and fault management;
- Annual Disaster management exercise;
- Support performed weekly only from 5:00 a.m. to 7:00 a.m.;
- Backups at application and database level for every major release;
- Failure/fault notification to Exchange for all production outages;
- Failure/fault notification to Exchange for all other outages lasting longer than ten (15) minutes

BEST servers are housed in a temperature and humidity controlled facility providing power system automatic failover, redundant power AC circuits, primary and fail over secondary ISP providers, automatic fire suppression devices, redundant network routers, 24 hours security guards and surveillance, router security and locked server racks. BEST Servers are backed up on a regularly scheduled backup schedule that can be recovered on request.

BEST support for servers will be available during normal business hours: 8:00 a.m. to 5:00 p.m. (Eastern Standard Time), Monday through Friday, except for State holidays. Scheduled maintenance and backup procedures will be performance as needed and will occur outside normal business hours.

The application servers will have backups created for every major revision made to the applications. The Exchange database servers will have backups created for every major revision made to the databases.

BEST will perform backups according to standards schedules defined by the Exchange. Application, database and server recorder will be the responsibility of BEST. Recovery may be requested by the BEST IT manager or designee. If recovery requires vendor assistance, BEST may contract these services to a vendor with the prior written approval of the Exchange IT Systems and Operations Team. Vendor costs associated with the recovery will be charged to the Exchange and included in its monthly bill.

Restoration requests must be requested through the BEST Lead or the BEST contact listed below if this lead has not been defined. Service restoration time will vary depending on the severity of the problem and the scope of the restoration (i.e. database table vs. full server).

BEST will upgrade and/or apply patches to the server hardware, operating systems and hosting software to maintain an OEM supported environment.

### **9.1.4.2 Service Level Objectives**

Recovery Time Objective for application recovery is 4 hours i.e. up to 4 hours of production data loss is possible based on their backup and recovery plan. Recovery Time Objective for Disaster recovery is recovering a Cold Site: 4 days(s) or less (specify amount) 96hours and based on overall State of Connecticut priorities. The Exchange and DSS agencies will be the data owner and be responsible for recovering their own data loss during an outage.

## **9.1.5 Storage Area Network Services**

### **9.1.5.1 Service Definition**

Storage Area Network Services provide centralized, highly-available, highly-scalable data storage for server systems through application and file servers to near-line mass storage for imaging and other data repositories. The services include storage, backup and archival area is provided over a wide range of hardware and software operating systems.

The following are available within Storage Area Network Services:

- Application Failover;
- Data Recovery Services;
- Sharing Data Access to/from storage
- SAN Software Capability;
- Storage Area Network Fabric (Fiber channel switches, Fiber Cabling etc.);
- Tape Library Connections;

Storage Area Network Services will produce the following key benefits:

- Server-less backups;
- Data is kept on the SAN;
- Server processing resources are still available to client systems
- Supporting faster data rates;

BEST provides a variety of storage, backup and archival through the user of a Storage Area Network (SAN) infrastructure. This technology is used to back up the servers, database, and content file for applications. There is a standard or normal backup and archival practice used that accommodates most applications needs. This process creates a primary copy, a mirrored copy, and copies the file to tape. This gives the options of a real time copy at set intervals of what is on the service and create a mirrored image for the unlikely need to restore from a failed drive on the Storage Area Network. The mirrored files are used to archive the data onto tape for onsite and offsite storage. These actions are considered a "best practice" and should meet all needs for the mission critical applications identified.

Exchange applications will be stored locally on the application services (s). Exchange shall provide BEST with an initial storage allocation based on current design within the Chargeback model. Additional storage needs for data; growth beyond the capacity of the targeted servers currently in used or special needs such as additional copies of files near-line or offline use may have additional changes. Such requested may be submitted to the BEST help desk.

### **9.1.5.2 Service Level Objectives**

We can add throughput requirements. 10 GB Fibre channel is recommended for SAN connections that will provide a network throughput of 2560 Mega Bytes/Sec.

For Storage Area Network Services, Exchange and BEST will leverage the process as defined within the Service Level Agreements set out in future documentation as mutually agreed;

### **9.1.6 Network Services**

BEST Network Services provides highly availability network services and support for Exchange Application Connectivity to the State of Connecticut Network. These services are provided over a wide range of hardware and software network systems.

The following are available within Network Services:

- Network Backbone Services
- Wide Area Network (WAN) Services;
- Virtual Private vLAN Network Services;
- Networking Services (DNS, DHCP);
- Network Management & Support;

#### **9.1.6.1 Network Backbone Services**

BEST Network team will provide a network connection of the Exchange application to the existing 10Gig Network CORE Backbone at BEST.

#### **9.1.6.2 Wide Area Network (WAN) Services**

BEST Networking will provide Wide Area Network (WAN) Network Connections to the following Agencies for the Exchange Application – they include:

- a) Department of Social Services (DSS)
- b) Department of Public Health (DPH)
- c) New Exchange Corporate Office at 280 Trumbull Street Hartford, CT

This WAN network is currently designed to support the network traffic of the State of Connecticut Agencies today. If there are additional users and or data payload growth required by the Exchange Application, BEST team reserves the right to chargeback any additional network switching, monitoring, and/or fiber equipment back to the Exchange program.

#### **9.1.6.3 vLAN Network Services**

BEST will provide Virtual Local Area (vLAN) Services to connect the Exchange Web, Application, and Database servers up to the BEST Network CORE Backbone and Internet.

BEST will also provide SAN Network Connectivity to UAT, Staging, and Production Servers for the Exchange Application.

#### **9.1.6.4 Internet ISP Services**

BEST will supply Internet Network Services through their ISP vendors for the Exchange application. These services will include:

- Exchange users will be able to access the Exchange application via State Intranet and Internet channels. Access to Exchange will be authorized as determined by Exchange/BEST security Standards.
- When users access the application via the Internet, BEST security will be incorporated to provide access to the Intranet. The Exchange will provide the same level of application security and data security that is currently provided when users access the application from within the State network, as set forth in Appendix B - CMS Data Security Controls and Appendix C - Compliance with IRS PUB 1075.
- Access to Exchange via the Internet will only be granted to users authorized to access Exchange according to Exchange/BEST standards.
- BEST is responsible for access issues caused by Internet Service Providers (ISPs)
- BEST will charge Exchange for Internet Access Fees based on # of Users and Data Payload usage of the Exchange Application. This is so BEST can reimburse the ISP vendors for Internet Access. If the user or data payload growth expands in the future. The BEST team may need to upgrade their Backbone Network to 40 Gig. The cost for the upgrade and new switches attributable to the Exchange will be charged back to Exchange. These costs are for Internet access provided by BEST through the ISP vendors.
- User authentication will occur at the application and database level when a user attempts to access Exchange via the Intranet. Network, application, and database authentication will occur for State network users as defined by the State Security standards
- Firewall services will be provided between DMZ Web servers and application servers to prevent unauthenticated users from accessing Exchange via the Internet. Firewall services upgrades in the Internet DMZ may be needed if the number of Exchange users increases or the Data Payload Increases. These upgrades will be charged back to Exchange

#### **9.1.7 Exchange Security Services**

##### **9.1.7.1 Service Definition**

Security Services provide support and services to prevent unauthorized visitors from accessing valuable BEST and Exchange resources and help BEST and Exchange comply with security and regulatory requirements by the State of Connecticut, CMS and the IRS through the use of firewall and intelligent network services. These solutions also include advanced monitoring and reporting, wide area and local network connectivity, network management and other networking services (DNS and DHCP). These services are provided over a wide range of hardware and software operating systems.

The following are available within Security Services:

- Network protection for inbound and outbound security threats;
- Managed firewall services;
- Protection from the latest security threats;

Security Services will produce the following key benefits:

- Manage inbound and outbound security threats;
- Notification of any firewall breaches;
- Notification of any change to firewall rules and policies (Given most breaches are a direct result of misconfiguration of firewall rules and policies)

BEST will provide a Firewall service that will ensure that all communications attempting to cross it meet the State of Connecticut's and the Exchange's security policies which shall include all requirements set forth by CMS and IRS as outlined in Appendices B and C to this MOU. These firewalls track and control communications, deciding whether to allow or reject communications based on security policies and rules. These firewalls not only will be designed primarily to provide access control to network resources but also to protect sensitive portions of the local area networks and servers.

The installation will be managed by BEST technical staff and have extensive logging and audit capability, to produce reports and security audits based on Exchange requirements which shall include all requirements set forth by CMS and IRS as outlined in Appendices B and C to this MOU.

#### **9.1.7.2 Service Level Objectives**

For Firewall/Network Services, Exchange and BEST will leverage the process as defined within the Service Level Agreements set out in future documentation as mutually agreed;

### **9.1.8 Infrastructure Security Services**

#### **9.1.8.1 Service Definition**

Infrastructure Security Services provide support and services to prevent unauthorized visitors from accessing valuable BEST and Exchange resources and help BEST and Exchange comply with security and regulatory requirements by the State of Connecticut, CMS and the IRS through the use of firewall and intelligent network services. These solutions also include advanced monitoring and reporting, wide area and local network connectivity, network management and other networking services (DNS and DHCP). These services are provided over a wide range of hardware and software operating systems.

The following are available within Infrastructure Security Services:

- Security network (configuration and topology), network traffic and communication systems
- Define security policy, processes, procedures, and implementation plan to meet requirements of the Exchange, CMS and the IRS;

- Maintain a standardized documentation of the entire IT infrastructure;
- Identity Management & Directory Services;
- Periodically test and audit the entire network security (Internet, Intranet and Extranet), update it regularly, and maintain an audit trail of all changes; and
- Security Incident Investigations.
- Data security – In addition, BEST will be responsible for collecting and implementing data encryption and security for IRS requirements and external accessed web services.

Infrastructure Security Services will produce the following key benefits:

- Single Sign-on;
- Undertake preventive measures, before corrective measures become necessary;
- Data reporting and transparency; and
- Architecture planning and design of enterprise database systems management and associated security elements.

#### **9.1.8.2 Service Level Objectives**

- BEST will setup the security audit logs according to Exchange provided security requirements.
- BEST will setup appropriate notification to Exchange based on security audit logs

### **9.1.9 Help Desk and Operational Services**

#### **9.1.9.1 Service Definition**

Helpdesk and Operational Services provide incident and problem management resolution for issues affecting the infrastructure environment and/or impacting downstream systems.

These services are provided over a wide range of hardware and software operating systems.

The following are available within Helpdesk and Operational Services:

- Incident & Problem Management;
- Data Center Operations;
- Technical Help Desk Services;
- Disaster Recovery Services; and
- Network Services.
- Telecommunications and phones systems are not covered in this MOU.

Helpdesk and Operational Services will produce the following key benefits:

- Tracking and resolution of problems impacting the Exchange infrastructure but not business operations;
- Incident tracking and management;
- Clear escalation path to resolve issues; and
- Centralized coordination of issue resolution.

BEST's Help Desk will provide HIX with a single point of contact for all information technology inquirers and problems related to the infrastructure and associated applications. Leveraging the existing BEST Help Desk, Exchange technical staff or other authorized Exchange personnel will contact the BEST Help Desk. The BEST Help Desk will determine if the issue can be resolved locally. If not, the BEST Help Desk will coordinate issue resolution.

Although BEST support services are available to Exchange during normal business hours, the BEST Help Desk is staffed 24 hours a day, seven days a week. In the event there is a question or problem after normal business hours, the BEST Help Desk is staffed 24 hours a day, seven days a week and can be reached by telephone. The Exchange application will be an option on the primary menu for the BEST helpdesk. The BEST Help Desk will record the incident in the incident tracking system and assign it to the appropriate BEST support group for resolution on the next business day.

BEST will follow the ITSM Incident process currently in place at BEST.

BEST is responsible for the infrastructure level and Deloitte is responsible for the application level, with Exchange having overall ownership for the delivery of a functioning system. Therefore, depending on the issue there may need to be coordination between BEST, Deloitte and the Exchange to fully resolve a helpdesk ticket.

Additionally, the BEST helpdesk is to be called only for technical issues by an authorized representative from the Exchange IT Systems and Operations Team. The BEST helpdesk is not for Exchange users, applying to the exchange, to call directly.

BEST Help Desk can be reached by phone: (860)-622-2300.

### **9.1.9.2 Service Level Objectives**

For Help Desk and Operational Services, Exchange and BEST will leverage the process as defined within the Service Level Agreements set out in future documentation as mutually agreed.

## **9.1.10 Change Management Process & Procedures**

### **9.1.10.1 Service Definition**

Change Management Procedures provide an approach to shifting/transitioning individuals, teams, and organizations from a current state to a desired future state.

The following are available within Change Management Procedures:

- Strategic changes, clear notification and approval;
- Operational changes (including Structural changes), clear notification and approval; and
- Technological changes, clear notification and approval.

Change Management Procedures will produce the following key benefits:

- Minimize the change impacts;
- Avoid distractions and conflicting priorities; and
- Documentation confirming changes in direction.

### **9.1.10.2 Change Impacting the 5ons (Scope, Schedule, Budget, Quality, and Benefits)**

This process covers the hand off for events impacting strategic or program level and the approval and acknowledgement of entry/exit criteria for 5ons changes. Exchange and BEST will leverage the process as defined within the Service Level Agreements set out in future documentation as mutually agreed;

### **9.1.10.3 Production Change Control**

The following change management procedures shall be in effect until superseded by a revised change management process and procedures.

BEST provides electronic means that Exchange will use to request all changes in the distributed systems UAT, staging and production environments. BEST technical resources will notify Exchange when to commence use of the formal change management process for the staging and production environments. While the hosting environment is under construction, an informal change process will be used which permits submission of change requests via e-mail to the BEST technical staff working on the installation.

BEST change Control must receive submission of the change requests by 12:00 p.m. (Eastern Standard Time), Monday and Wednesday for implementation on the following day. Production changes are done prior to 7:00 a.m. or after 6:00 p.m. (Eastern Standard Time). Staging changes can be done anytime during the day.

Change requests for the applications, databases and hosting environments must be submitted via a request process mutually agreed by both parties.

Any program code that is identified in the change request must remain untouched from the time of the change request. If the timestamp of the program code is after the submission of request, BEST reserves the right to deny the change request or push until the next code/build drop date. These programs must be thoroughly tested in the staging environment prior to a request to move into production. Database changes will be provided by Exchange or Exchange designee, or a support service provider working under the direction of Exchange, through the use of a data definition language consistent with the database software utilized by the application. Approval to move code from one environment to another will require joint approval from Exchange IT Systems and Operations Team and from BEST group or a BEST designee.

UAT, Staging/Testing and Production environments will be maintained on the BEST managed hardware.

All change requests must identify a method to determine if the move to production is successful, such as successful criteria, a day-of implementation plan and a documented back out plan. This could consist of a short procedure or a notification to the developer via email requiring their verification of success, for example, distribution group email.

All change requests must contain back out procedures in the event that problems occur.

If multiple servers are impacted in a request for a production move, the change request must document whether the updates on the different servers are mutually exclusive. Any change request outside the schedule timeframe must be requested through the Help Desk as an EMERGENCY change request.

#### **9.1.10.4 Release Management**

Exchange and BEST will utilize the BEST Release Management Process currently in place.

#### **9.1.10.5 Service Level Objectives**

For Change Management Process & Procedures, Exchange and BEST will leverage the process as defined within the Service Level Agreements set out in future documentation as mutually agreed.

### **10. CONFIDENTIALITY DEFINITIONS**

**Confidential Information:** Any name, number or other information that may be used, alone or in conjunction with any other information, to identify a specific individual including, but not limited to, such individual's name, date of birth, mother's maiden name, motor vehicle operator's license number, Social Security number, employee identification number, employer or taxpayer identification number, alien registration number, government passport number, health insurance identification number, demand deposit account number, savings account number, credit card number, debit card number or unique biometric data such as fingerprint, voice print, retina or iris image, or other unique physical representation. Without limiting the foregoing, Confidential Information shall also include any information that the Exchange, BEST or DAS classifies as "confidential" or "restricted." Confidential Information shall not include information that may be lawfully obtained from publicly available sources or from federal, state, or local government records which are lawfully made available to the general public

**Confidential Information Breach:** Generally, an instance where an unauthorized person or entity accesses Confidential Information in any manner, including but not limited to the following occurrences: (1) any Confidential Information that is not encrypted or protected is misplaced, lost, stolen or in any way compromised; (2) one or more third parties have had access to or taken control or possession of any Confidential Information that is not encrypted or protected without prior written authorization from the State; (3) the unauthorized acquisition of encrypted or protected Confidential Information together with the confidential process or key that is capable of compromising the integrity of the Confidential Information; or (4) if there is a substantial risk of identity theft or fraud to the Exchange, BEST, any Contractor performing under this Agreement, DAS or the State.

## **11. PROTECTION OF CONFIDENTIAL INFORMATION**

### **11.1 DUTY TO PROTECT**

Exchange and BEST at their own expense, have a duty to and shall protect from a Confidential Information Breach any and all Confidential Information which they come to possess or control, wherever and however stored or maintained, in a commercially reasonable manner in accordance with current industry standards.

### **11.2 DATA SECURITY PROGRAM**

Exchange and BEST shall develop, implement and maintain a comprehensive data security program for the protection of Confidential Information. The safeguards contained in such program shall be consistent with and comply with the safeguards for protection of Confidential Information, and information of a similar character, as set forth in all applicable federal and state law and as set forth in Appendix A - CMS Security Controls and in Appendix B - Compliance with IRS Publication 1075 of this Agreement and with the written policies of the Exchange, DAS or the State concerning the confidentiality of Confidential Information. Such data-security program shall include, but not be limited to, the following:

**11.2.1** A security policy for employees related to the storage, access and transportation of data containing Confidential Information;

**11.2.2** Reasonable restrictions on access to records containing Confidential Information, including access to any locked storage where such records are kept;

**11.2.3** A process for reviewing policies and security measures at least annually;

**11.2.4** Creating secure access controls to Confidential Information, including but not limited to passwords; and

**11.2.5** Encrypting of Confidential Information that is stored on laptops, portable devices or being transmitted electronically.

### **11.3 MANDATORY REPORTING.**

The Exchange or BEST as applicable shall notify DAS and the Connecticut Office of the Attorney General as soon as practical, but no later than twenty-four (24) hours, after they become aware of or suspect that any Confidential Information which the Exchange or BEST or that any contractor of the Exchange or BEST performing work under this Agreement has come to possess or control has been subject to a Confidential Information Breach. Upon discovering a breach of HIPAA protected data, a representative of the Exchange or BEST, as applicable, shall notify, affected individuals, without unreasonable delay, and in no case later than 60 days from date of discovery of the breach. If the breach affects less than 500 residents of the state, notice of breach may be made to the Secretary of HHS on an annual basis. If the breach affects more than 500 residents, notice to the Secretary of HHS must be made without

unreasonable delay, and in no case later than 60 days. In addition if the breach affects more than 500 residents of the state, notice must be provided to prominent media outlets serving the state without unreasonable delay and in no case later than 60 days. Upon discovering a possible improper inspection or disclosure of FTI, including breaches and security incidents by a federal employee, a state employee, or any other person, the representative of the Exchange or BEST, as applicable shall notify the office of the appropriate Special Agent-in-Charge, Treasury Inspector General for Tax Administration (TIGTA) and the IRS with 24 hours.

#### **11.4 PROTECTION PLAN AND CREDIT MONITORING.**

If a Confidential Information Breach has occurred, the Exchange or BEST, as applicable shall be responsible for presenting within three (3) business days after the notification, a credit monitoring and protection plan to the Commissioner of Administrative Services and the Connecticut Office of the Attorney General, for review and approval. Such credit monitoring or protection plan shall be made available by the Exchange or BEST at its own cost and expense to all individuals affected by the Confidential Information Breach. Such credit monitoring or protection plan shall include, but is not limited to reimbursement for the cost of placing and lifting one (1) security freeze per credit file pursuant to Connecticut General Statutes § 36a-701a. Such credit monitoring or protection plans shall be approved by the State in accordance with this Section and shall cover a length of time commensurate with the circumstances of the Confidential Information Breach. Any contractors' costs and expenses for the credit monitoring and protection plan shall not be recoverable from the Exchange, BEST, DAS, any State of Connecticut entity or any affected individuals.

#### **11.5 RESPONSIBILITY OF CONTRACTORS.**

The Exchange and BEST shall incorporate the requirements of this Section in all contracts requiring each Contractor Party to safeguard Confidential Information in the same manner as provided for in this Section.

#### **11.6 IMPACT ON HIPAA.**

Nothing in this Section shall supersede in any manner the Exchange's or BEST's obligations pursuant to the Health Insurance Portability and Accountability Act of 1996 or any provisions of this Agreement concerning the obligations of the Exchange as a business associate (as such term is defined in 45 C.F.R. § 160.103) of the Department.

### **12. MODIFICATION AND TERMINATION**

#### **12.1 TERMINATION FOR MATERIAL BREACH**

This MOU or any Project Agreement can be terminated at any time for material breach upon provision of written notice and a reasonable opportunity to cure.

## **12.2 TERMINATION FOR CONVENIENCE**

This agreement may be cancelled or terminated without cause by either party by giving (90) calendar days advance written notice to the other party. Such notification shall state the effective date of termination or cancellation and include any final performance and/or payment invoicing instructions/requirements. All reasonable efforts shall be made to minimize disruption of work under existing Project Agreements.

## **12.3 LOSS OF FUNDING**

It is mutually agreed that if the Exchange does not have sufficient funds and the State Budget of the current year and/or any subsequent years covered under this Agreement does not appropriate sufficient funds for the Exchange, this Agreement shall be of no further force and effect. In this event, the Exchange shall have no liability to pay any funds whatsoever to BEST and BEST shall not be obligated to perform any provisions of this Agreement for which they are not reimbursed. If funding for any fiscal year is reduced or deleted by the State Budget for purposes of this program, the Exchange shall have the option to either cancel this Agreement with no liability occurring to the BEST, or with BEST's agreement amend the MOU to reflect the reduced amount of funding.

## **13. ENTIRE AGREEMENT/MODIFICATION**

This MOU constitutes the entire agreement between the parties and may be amended only in writing signed by all parties. Any and all amendments must be made in writing and must be agreed to and executed by the parties before becoming effective.

## **14. INTELLECTUAL PROPERTY**

This MOU is in support of the Exchange's implementation of the Patient Protection and Affordable Care Act of 2010, and is subject to the certain property rights provisions of the Code of Federal Regulations and a Grant from the Department of Health and Human Services, Centers for Medicare & Medicaid Services. This MOU is subject to, and incorporates by reference, 45 CFR 74.36 and 45 CFR 92.34 governing rights to intangible property. Intangible property includes but is not limited to: computer software; patents, inventions, formulae, processes, designs, patterns, trade secrets, or know-how; copyrights and literary, musical, or artistic compositions; trademarks, trade names, or brand names; franchises, licenses, or contracts; methods, programs, systems, procedures, campaigns, surveys, studies, forecasts, estimates, customer lists, or technical data; and other similar items. BEST may copyright any work that is subject to copyright and was developed, or for which ownership was purchased, under this MOU. However, BEST must deliver all intangible property, including but not limited to, intellectual property, to the Exchange in a manner that ensures the Centers for Medicare & Medicaid Services of the Department of Health and Human Services, and the Exchange obtains a royalty-free, nonexclusive and irrevocable right to reproduce, publish, or otherwise use the work for Federal of Exchange purposes, and to authorize others to do so. Federal purposes include the purpose of administering state exchanges under the Affordable Care Act of 2010. BEST is further subject to applicable regulations governing patents and inventions, including those issued by the Department of Commerce at 37 CFR Part 401.

## **15. INSURANCE**

Each party shall maintain its own liability and crime insurance and fidelity bond insurance in amounts deemed appropriate for its operations. Such insurance shall provide coverage for negligent acts, errors, or omissions and provide protection against bodily injury or property damage claims. It is expressly understood that each party shall be solely responsible for its own actions and such insurance shall not extend to protect any other party.

## **16. APPLICATION OF LAW**

This MOU and any Project Agreements shall be governed and construed under the laws of the State of Connecticut, United States of America, without regard to its principles of conflicts of law. The parties will consult with each other and attempt to resolve disputes or misunderstandings that arise in the administration of this MOU or any Project Agreement informally. In the event that informal attempts at resolution are not successful, the parties agree that all claims or actions, related to, or arising out of, activities described in this MOU or any Project Agreement shall be brought only in the courts of the State of Connecticut or the United States having jurisdiction in Hartford County, State of Connecticut.

## **17. LANGUAGE OF EXECUTION**

Although all languages are deemed equally authentic, should this MOU be executed in more than one language, the English version shall control in the event of inconsistency in meaning or interpretation of terms. All notices, communications and proceedings under this MOU shall be delivered/conducted in English.

## **18. MULTIPLE COUNTERPARTS**

This MOU may be executed in any number of counterparts and by facsimile signature. All of such counterparts taken together shall, for all purposes, constitute one MOU binding upon all of the parties.

## **ACCEPTANCES AND APPROVALS**

**Department of Administrative Services**

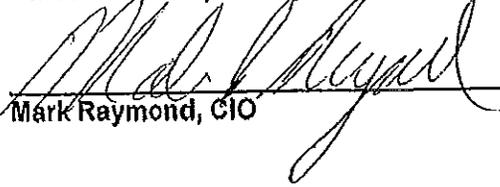
**Date**

\_\_\_\_\_  
Donald J. DeFronzo, Commissioner

\_\_\_\_\_

Bureau of Enterprise Systems and Technology

Date

  
\_\_\_\_\_  
Mark Raymond, CIO

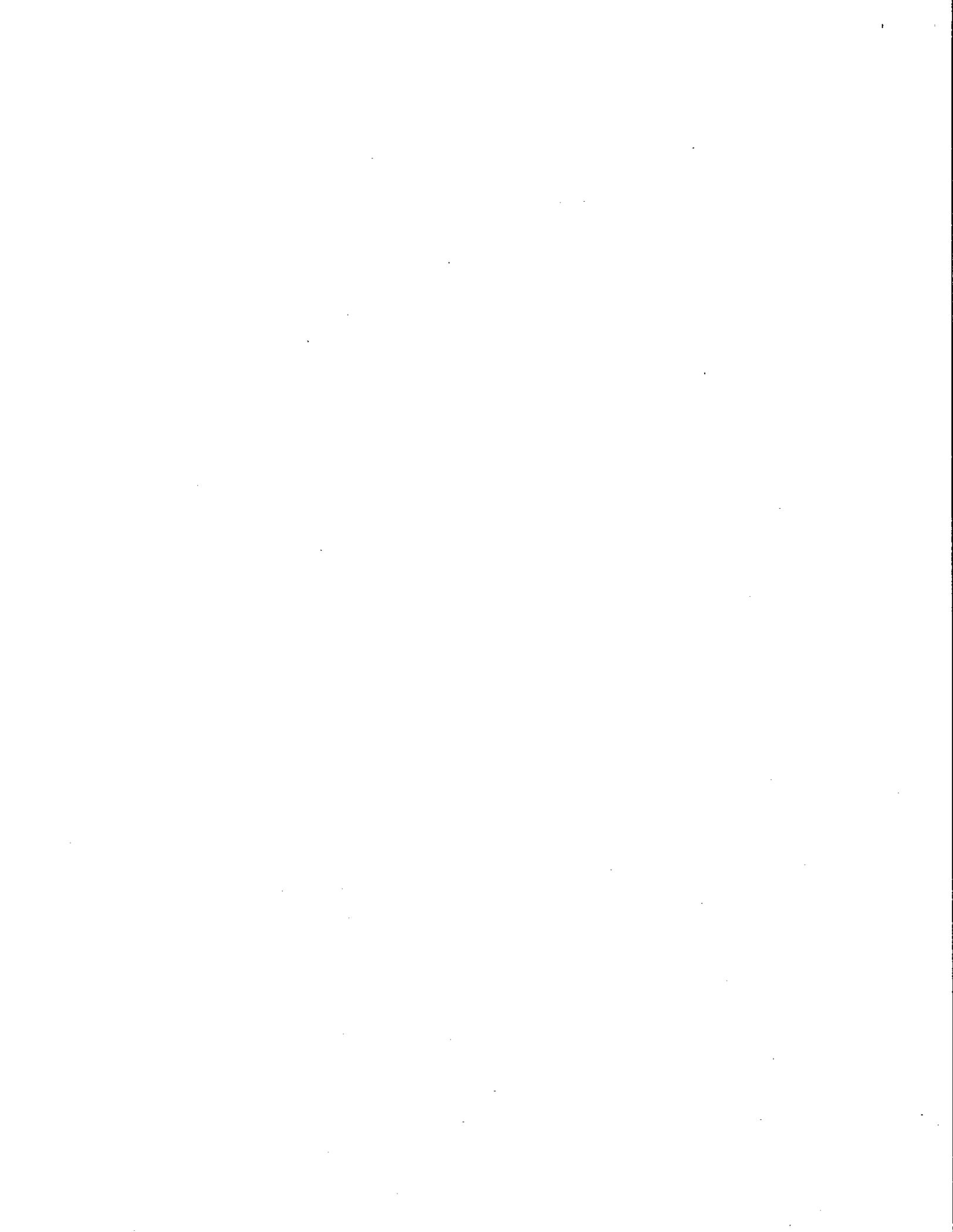
10/3/13

Connecticut Health Information Exchange  
dba Access Health CT

Date

  
\_\_\_\_\_  
Kevin J. Counihan, CEO

8/28/13



## CMS Security Control Detail

BEST will ensure that the information system routes all remote accesses through a limited number of managed access control points.

(AC- 17.3)

BEST will authorize the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system.

(AC-17(4) – Enhancement)

BEST will prohibit the connection of portable and mobile devices [e.g., notebook computers, personal digital assistants (PDA), cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations] to Exchange information systems unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization:

- a. Employs an approved method of cryptography (see SC-13) to protect information residing on portable and mobile information devices, and utilizes whole-disk encryption solution for laptops;
- b. Monitors for unauthorized connections of mobile devices to information systems;
- c. Enforces requirements for the connection of mobile devices to information systems;
- d. Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction;
- e. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and
- f. Protects the storage and transmission of information on portable and mobile information devices with activities such as scanning the devices for malicious code, virus protection software.

(AC-19)

BEST will prohibit the use of external information systems, including but not limited to, Internet kiosks, personal desktop computers, laptops, tablet personal computers, personal digital assistant (PDA) devices, cellular telephones, facsimile machines, and equipment available in hotels or airports to store, access, transmit, or process sensitive information (such as FTI or Privacy Act protected information), unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization establishes strict terms and conditions for their use. The terms and conditions shall address, at a minimum:

- a. The types of applications that can be accessed from external information systems;
- b. The maximum FIPS 199 security category of information that can be processed, stored, and transmitted;
- c. How other users of the external information system will be prevented from accessing federal information;
- d. The use of virtual private networking (VPN) and firewall technologies;

## CMS Security Control Detail

- e. The use of and protection against the vulnerabilities of wireless technologies;
- f. The maintenance of adequate physical security controls;
- g. The use of virus and spyware protection software; and
- h. How often the security capabilities of installed software are to be updated.

(AC-20)

BEST will perform an assessment to ensure that:

- (i) the organization prohibits the use of external information systems to store, access, transmit, or process sensitive information unless explicitly authorized, in writing, by the CIO;
- (ii) if authorized, the organization identifies individuals authorized to: – access the information system from the external information systems; – process, store, and/or transmit organization-controlled information using the external information systems;
- (iii) if authorized, the terms and conditions address, at a minimum: – the types of applications that can be accessed from external information systems; – the maximum FIPS-199 security category of information that can be processed, stored, and transmitted; – how other users of the external information system will be prevented from accessing federal information; – the use of virtual private networking (VPN) and firewall technologies; – the use of and protection against the vulnerabilities of wireless technologies; – the maintenance of adequate physical security controls; – the use of virus and spyware protection software; and – how often the security capabilities of installed software are to be updated.
- (iv) The organization meets all the requirements specified in the applicable implementation standard(s); and
- (v) Only organizational owned computers and software are used to process, access, and store PII.

(AC-20.1)

BEST will:

- a. Designate individuals authorized to post information onto an information system that is publicly accessible;
- b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
- c. Review the proposed content of publicly accessible information for nonpublic information prior to posting onto the information system;
- d. Review the content on the publicly accessible information system for nonpublic information monthly; and
- e. Remove nonpublic information from the publicly accessible information system, if discovered.

(AC-22)

BEST will:

- a. Review and analyze information system audit records regularly for indications

## CMS Security Control Detail

of inappropriate or unusual activity, and report findings to designated organizational officials;

- b. Adjust the level of audit review, analysis, and reporting within the information system when there is a change in risk to CMS operations, CMS assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.
- c. Ensure that all FTI requests for return information, including receipt and/or disposal of returns or return information, shall be maintained in a log.

(AU-6)

BEST will:

- a. Provide the results of the security control assessment within every three hundred sixty-five (365) days, in writing, to the Exchange who is responsible for reviewing the assessment documentation and updating system security documentation where necessary to reflect any changes to the system.
- b. Implement standards for a security assessment that will include an annual security assessment requirement mandated by OMB requires all CMSRs attributable to a system or application to be assessed over a 3-year period. To meet this requirement, a subset of the CMSRs shall be tested each year so that all security controls are tested during a 3-year period. In addition, the Exchange will notify the CISO within thirty (30) days whenever updates are made to system security authorization artifacts or significant role changes occur (e.g., Business Owner, System Developer/Maintainer, ISSO).

(CA-2)

BEST will:

- a. Authorizes connections from the Exchange information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements;
- b. Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and
- c. Monitors the information system connections on an ongoing basis verifying enforcement of security requirements.

(CA-3)

BEST will update the security authorization:

- a. At least every three (3) years;
- b. When substantial changes are made to the system;
- c. When changes in requirements result in the need to process data of a higher sensitivity;
- d. When changes occur to authorizing legislation or federal requirements;
- e. After the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization; and
- f. Prior to expiration of a previous security authorization.

## CMS Security Control Detail

BEST will ensure that owners of FTI shall accredit the security controls used to protect FTI before initiating operations. This shall be done for any infrastructure associated with FTI. The authorization shall occur every three (3) years or whenever there is a significant change to the control structure. A senior agency official shall sign and approve the authorization.

(CA- 6)

BEST will establish a continuous monitoring strategy and implement a continuous monitoring program that includes:

- a. A configuration management process for the information system and its constituent components;
- b. A determination of the security impact of changes to the information system and environment of operation;
- c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and
- d. Reporting the security state of the information system to appropriate organizational officials within every three-hundred-sixty-five (365) days.

(CA-7)

BEST will, after the information system is changed, check the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.

(CM- 4.2)

BEST will define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system. Records reflecting all such changes shall be generated, reviewed, and retained.

(CM-5)

BEST will:

- a. Establish and document mandatory configuration settings for information technology products employed within the information system using the latest security configuration guidelines listed in Implementation Standard 1 that reflect the most restrictive mode consistent with operational requirements;
- b. Implement the configuration settings;
- c. Identify, document, and approve exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements;
- d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures; and
- e. Establish mandatory configuration settings for systems that receive, store, process and transmit FTI using the Safeguards Computer Security Evaluation Matrices (SCSEMs).

(CM-6)

BEST will ensure that it develops, documents, and maintains an inventory of information system components that:

- a. Accurately reflects the current information system;

## CMS Security Control Detail

b. Is consistent with the authorization boundary of the information system;  
c. Is at the level of granularity deemed necessary for tracking and reporting;  
d. Includes manufacturer, model/type, serial number, version number, location (i.e., physical location and logical position within the information system architecture), and ownership; and  
e. Is available for review and audit by designated organizational officials.  
(CM-8)

BEST will update the inventory of information system components as an integral part of component installations, removals, and information system updates.  
(CM-8.1)

BEST will verify that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.  
(CM-8.5)

BEST will:  
a. Conduct backups of user-level information contained in the information system in accordance with the frequency specified in Implementation Standard 1;  
b. Conduct backups of system-level information contained in the information system in accordance with the frequency specified in Implementation Standard 1;  
c. Conduct backups of information system documentation including security-related documentation and other forms of data, including paper records; and  
d. Protects the confidentiality and integrity of Exchange backup information at the storage location.  
(CP-9)

BEST will ensure that:  
a. The information system uses multifactor authentication for network access to privileged accounts.  
b. For FTI data: Two-factor authentication is required whenever FTI is being accessed from an alternative work location or if accessing FTI via agency's web portal by an employee or contractor.  
(IA-2.1)

BEST will ensure that the information system uses multifactor authentication for network access to non-privileged accounts.  
(IA-2.2)

BEST will ensure that the information system uses multifactor authentication for local access to privileged accounts.  
(IA-2.3)

BEST will ensure that the organization manages information system identifiers for users and devices by:  
a. Receiving authorization from a designated organizational official to assign a user or device identifier;  
b. Selecting an identifier that uniquely identifies an individual or device;  
c. Assigning the user identifier to the intended party or the device identifier to the

## CMS Security Control Detail

intended device;

- d. Preventing reuse of user or device identifiers until all previous access authorizations are removed from the system, including all file accesses for that identifier but not before a period of at least three hundred sixty-five (365) days has expired; and
- e. Disabling the user identifier after the time period of inactivity specified in Implementation Standard 1 and deleting disabled accounts during the annual re-certification process.

(IA-4)

BEST will ensure that it manages information system authenticators for users and devices by:

- a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;
- b. Establishing initial authenticator content for authenticators defined by the organization;
- c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
- d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
- e. Changing default content of authenticators upon information system installation;
- f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate);
- g. Changing/refreshing password authenticators as defined organizational password policy;
- h. Protecting authenticator content from unauthorized disclosure and modification; and
- i. Requiring users to take, and having devices implement, specific measures to safeguard authenticators.

(IA-5)

BEST will develop, disseminate, and review/update within every three-hundred-sixty-five (365) days:

A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

Ensure that all FTI Policies and procedures must cover both physical and information security relative to the protection of FTI.

(IR-1)

Ensure that it tests and/or exercises the incident response capability for the information system annually using reviews, analyses, and simulations to determine the incident response effectiveness and documents the results. For FTI: Include procedures to exercise responding to unauthorized FTI access and reporting unauthorized FTI access to IRS and TIGTA.

## CMS Security Control Detail

(IR-3)

BEST will ensure that it tracks and documents information system security incidents.

(IR-5)

BEST will :

- a. Develop an incident response plan that
  - Provides the organization with a roadmap for implementing its incident response capability;
  - Describes the structure and organization of the incident response capability;
  - Provides a high-level approach for how the incident response capability fits into the overall organization;
  - Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
  - Defines reportable incidents;
  - Provides metrics for measuring the incident response capability within the organization.
  - Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
  - Is reviewed and approved by designated officials within the organization;
- b. Distributes copies of the incident response plan to incident response personnel and organizational elements;
- c. Reviews the incident response plan within every three-hundred-sixty-five (365) days;
- d. Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and
- e. Communicates incident response plan changes to incident response personnel and organizational elements.

BEST will ensure that for FTI it will develop, document, and maintain a current incident response plan that describes the structure and organization of the incident response capability and includes incident response procedures specific to FTI.

(IR-8)

BEST will perform an assessment to ensure that it:

- (i) Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
- (ii) The organization controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
- (iii) The organization requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for offsite maintenance or repairs;
- (iv) The organization sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and
- (v) The organization checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

(MA- 2.1)

BEST will inspect all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications.

(MA-3(1) – Enhancement)

## CMS Security Control Detail

BEST will check all media containing diagnostic and test programs for malicious code before the media are used in the information system.

(MA-3(2) – Enhancement)

BEST will prohibit non-local system maintenance unless explicitly authorized, in writing, by the Exchange CIO or his/her designated representative. If authorized, BEST:

- a. Monitors and controls non-local maintenance and diagnostic activities;
- b. Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;
- c. Employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;
- d. Maintains records for non-local maintenance and diagnostic activities; and
- e. Terminates all sessions and network connections when non-local maintenance is completed.

(MA-4)

BEST will ensure that it:

1. Sanitizes information system media containing sensitive information (such as FTI or Privacy Act protected information) using National Security Agency (NSA) guidance ([www.nsa.gov/ia/government/mdg.cfm](http://www.nsa.gov/ia/government/mdg.cfm)) and NIST SP 800-88, Guidelines for Media Sanitization; and
2. Electronic media containing FTI is not made available for reuse by other offices or released for destruction without first being subject to electromagnetic erasing. If reuse is not intended, the electronic media should be destroyed by BEST. Whenever physical media leaves the physical or systemic control of the agency for maintenance, exchange or other servicing, any FTI on it must be cleared completely by overwriting all data tracks a minimum of three times.

(MP- 6.5)

BEST will implement controls to:

- Inventory physical access devices within every three hundred sixty-five (365) days.
- Change combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated.

(PE-3)

BEST will ensure that it:

1. Controls physical access to information system distribution and transmission lines within organizational facilities.

(PE-4)

BEST will:

Control physical access to information system output devices to prevent unauthorized individuals from obtaining the output.  
Ensure that for FTI: Output from printers and fax machines should be in a controlled area and secured when not in use. Physical access to monitors

## CMS Security Control Detail

<p>displaying FTI should be controlled to prevent unauthorized access to the display output.</p> <p>(PE-5)</p>
<p>BEST will implement standards and controls to:</p> <ol style="list-style-type: none"> <li>a. Evaluate the level of alert for temperature and humidity controls and follow prescribed guidelines for that alert level.</li> <li>b. Alert the Exchange of possible loss of service and/or media resulting from problems that arise from a failure of temperature and humidity controls.</li> <li>c. Report damage and provide remedial action for any problems that may arise from a failure of temperature and humidity controls. BEST will also implement a contingency plan to mitigate the risk of loss of service and/or media.</li> </ol> <p>(PE-14)</p>
<p>BEST will implement controls to assesses as feasible, the effectiveness of security controls at alternate work sites</p> <p>(PE-17)</p>
<p>BEST will:</p> <ol style="list-style-type: none"> <li>a. Screen individuals prior to authorizing access to the information system; and</li> <li>b. Rescreen individuals periodically, consistent with the criticality/sensitivity rating of the position.</li> <li>c. Ensure that for FTI: Individuals must be screened before authorizing access to information systems and devices containing FTI.</li> </ol> <p>(PS-3)</p>
<p>BEST will:</p> <ol style="list-style-type: none"> <li>a. Ensures that individuals requiring access to information or information systems sign appropriate access agreements prior to being granted access; and</li> <li>b. Review/update the access agreements as part of the system security authorization or when a contract is renewed or extended.</li> <li>c. Ensure that for FTI: Agencies must review information system access authorizations and initiate appropriate actions when personnel are reassigned or transferred to other positions within the organization.</li> </ol> <p>(PS-6)</p>
<p>BEST will:</p> <ol style="list-style-type: none"> <li>a. Scan for vulnerabilities in the information system and hosted applications within every ninety (90) days and when new vulnerabilities potentially affecting the system/applications are identified and reported;</li> <li>b. Employ vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for: – Enumerating platforms, software flaws, and improper configurations; – Formatting and making transparent, checklists and test procedures; and – Measuring vulnerability impact;</li> <li>c. Analyze vulnerability scan reports and results from security control assessments; d. Remediate legitimate vulnerabilities based on the Business Owner's risk prioritization in accordance with an organizational assessment of risk;</li> <li>d. Share information obtained from the vulnerability scanning process and security</li> </ol>

## CMS Security Control Detail

control assessments with designated personnel throughout the organization on a "need to know" basis to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).; and

e. Scan systems containing FTI quarterly to identify any vulnerability in the information system.

(RA-5)

BEST will employ vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.

(RA- 5.1)

BEST will include the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards:

- a. Security functional requirements/specifications;
- b. Security-related documentation requirements; and
- c. Developmental and evaluation-related assurance requirements.

(SA-4)

BEST will:

- a. Obtain, protect as required, and make available to authorized personnel, administrator documentation for the information system that describes:
  - Secure configuration, installation, and operation of the information system;
  - Effective use and maintenance of security features/functions; and
  - Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; and
- b. Obtain, protect as required, and make available to authorized personnel, user documentation for the information system that describes:
  - User-accessible security features/functions and how to effectively use those security features/functions;
  - Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and
  - User responsibilities in maintaining the security of the information and information system; and
- c. Document attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.

(SA- 5)

BEST will incorporate flaw remediation into the organizational configuration management process.

(SC-2)

BEST will ensure that the information system protects against or limits the effects of the following types of denial of service attacks defined on the following sites or in the following documents:

- a. SANS Organization [www.sans.org/dosstep](http://www.sans.org/dosstep);
- b. SANS Organization's Roadmap to Defeating DDoS [www.sans.org/dosstep/roadmap.php](http://www.sans.org/dosstep/roadmap.php); and

## CMS Security Control Detail

c. NIST CVE List <http://checklists.nist.gov/home.cfm>.

(SC-5)

BEST will implement standards to:

- Ensure that access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.
- Utilize stateful inspection/application firewall hardware and software.
- Utilize firewalls from at least two (2) different vendors at the various levels within the network to reduce the possibility of compromising the entire network.

(SC-7)

BEST will physically allocate publicly accessible Exchange information system components to separate subnetworks with separate physical network interfaces.

(SC-7.1)

BEST will ensure that it prevents public access into the organization's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices.

(SC-7.2)

BEST will ensure that it limits the number of access points to the information system (e.g., prohibiting desktop modems) to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.

(SC-7.3)

BEST will:

- a. Implement a managed interface for each external telecommunication service;
- b. Establish a traffic flow policy for each managed interface;
- c. Employ security controls as needed to protect the confidentiality and integrity of the information being transmitted;
- d. Document each exception to the traffic flow policy with a supporting mission/business need and duration of that need;
- e. Review exceptions to the traffic flow policy within every three-hundred-sixty-five (365) days; and
- f. Remove traffic flow policy exceptions that are no longer supported by an explicit mission/business need.

(SC-7.4)

BEST will ensure that the information system, at managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).

(SC-7.5)

BEST will prevent the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.

(SC-7.6)

BEST will ensure that the information system prevents remote devices that have

## CMS Security Control Detail

established a non-remote connection with the system from communicating outside of that communications path with resources in external networks.

(SC-7.7)

BEST will correct identified information system flaws on production equipment in a timeframe based on the National Vulnerability Database (NVD) Vulnerability Severity Rating of the flaw: flaws rated as High severity within seven (7) calendar days; Medium severity within fifteen (15) calendar days; and all others within thirty (30) calendar days.

(SI-2)

BEST will centrally manage the flaw remediation process and install software updates automatically.

(SI- 2.1)

BEST will employ automated mechanisms monthly to determine the state of information system components with regard to flaw remediation.

(SI- 2.2)

BEST will:

1. Employ malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code:
  - a. Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or
  - b. Inserted through the exploitation of information system vulnerabilities;
2. Update malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with configuration management policy and procedures;
3. Configure malicious code protection mechanisms to:
  - a. Perform critical system file scans during system boot, information system scans using the frequency specified in Implementation Standard 1, and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and
  - b. Block and quarantine malicious code and send alert to administrator in response to malicious code detection; and
4. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

(SI-3)

BEST will centrally manage malicious code protection mechanisms.

(SI-3.1)

## CMS Security Control Detail

BEST will ensure that the information system automatically updates malicious code protection mechanisms (including signature definitions).

(SI- 3.2)

BEST will ensure that the information system prevents non-privileged users from circumventing malicious code protection capabilities.

(SI- 3.3)

BEST will implement controls for:

- Information system detection of unauthorized changes to software and information.
- Reassessing the integrity of software and information by performing daily integrity scans of the information system.

(SI-7 & SI-7.1)

BEST will verify that all Access Health CT infrastructure components are hardened to IRS Computer Security Evaluation Matrix (SCSEM) requirements. BEST will provide and maintain documentation demonstrating that the applicable SCSEM test has been performed prior to any new infrastructure component that is released for service in the Access Health CT Staging or Production environments. BEST will also be responsible for ensuring that each component is maintained in compliance.

(SI-7)

Additional Controls Required by IRS Publication 1075 - Protection of FTI in Virtual Environment

Additional Controls Required by IRS Publication 1075 - Protection of FTI in Voice Over IP (VOIP) Networks

Additional Controls Required by IRS Publication 1075 - Protection of FTI in Cloud Computing Environments)

BEST will verify that any Virtual Hosts that host Access Health CT virtual machines are hardened to IRS SCSEM requirements. BEST will provide and maintain documentation demonstrating that the applicable SCSEM test has been performed prior to any new Virtual Host that is released for service in the Access Health CT Staging or Production environments. BEST will also be responsible for ensuring that each component is maintained in compliance.

(General Requirement)

## APPENDIX B – COMPLIANCE WITH IRS PUB 1075

### I. PERFORMANCE

In performance of this contract, BEST agrees to comply with and assume responsibility for compliance by BEST employees with the following requirements:

- (1) All work will be performed under the supervision of BEST or BEST's responsible employees.
- (2) Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this MOA. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this MOA. Disclosure to anyone other than an officer or employee of BEST, or the authorized representative of the Exchange, who shall use this data only for the purposes of this MOA is prohibited.
- (3) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output and products will be given the same level of protection as required for the source material.
- (4) BEST certifies that the data processed during the performance of this MOA will be completely purged from all data storage components of BEST's computer facility, and no output will be retained by the BEST at the time the work is completed. If immediate purging of all data storage components is not possible, BEST certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.
- (5) Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the Exchange for appropriate handling. When this is not possible, BEST will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the Exchange with a statement containing the date of destruction, description of material destroyed, and the method used.
- (6) All computer systems receiving, processing, storing, or transmitting Federal tax information must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Federal tax information.
- (7) No work involving Federal tax information furnished under this MOA will be subcontracted without prior written approval of the Exchange or IRS.
- (8) BEST will maintain a list of employees authorized access. Such list will be provided to the Exchange and, upon request, to the IRS reviewing office.

(6) The Exchange will have the right to void the MOA if BEST fails to provide the safeguards described above.

## II. CRIMINAL/CIVIL SANCTIONS

(1) Each officer or employee of the Exchange or BEST to whom returns or return information is or may be disclosed shall be notified in writing by Exchange or BEST that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as five years, or both, together with the costs of prosecution. The Exchange or BEST shall also notify each such officer and employee that any such unauthorized future disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than \$1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRC Sections 7213 and 7431 and set forth at 26 CFR 301.6103(n) -1.

(2) Each officer or employee of the Exchange or BEST to whom returns or return information is or may be disclosed shall be notified in writing by the Exchange or BEST that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this MOU. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this MOU. Inspection by or disclosure to anyone without an official need to know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000.00 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. The Exchange or BEST shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of \$1,000.00 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. The penalties are prescribed by IRC Sections 7213A and 7431.

(3) Additionally, it is incumbent upon BEST to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to BEST by 5 U.S.C. 552a(m)(1), provides that any officer or employee of BEST, who by virtue of his/her employment or official position, has possession of or access to Exchange records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or entity not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.

(4) Granting BEST access to FTI must be preceded by certifying that each individual understands the Exchange's security policy and procedures for safeguarding IRS information. BEST must maintain its authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the Exchange's files for review. As part of the certification and at least annually afterwards, contractors should be advised of the provisions of IRC Sections 7431, 7213, and 7213A (see Exhibit 6, *IRC Sec. 7431 Civil Damages for Unauthorized Disclosure of Returns and Return Information* and Exhibit 5, *IRC Sec. 7213 Unauthorized Disclosure of Information*). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. For both the initial certification and the annual certification, BEST should sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

### III. INSPECTION

The IRS and the Exchange shall have the right to send its officers and employees into BEST's facilities for inspection of the facilities and operations provided for the performance of any work under this MOA. On the basis of such inspection, specific measures may be required in cases where BEST is found to be noncompliant with contract safeguards.